

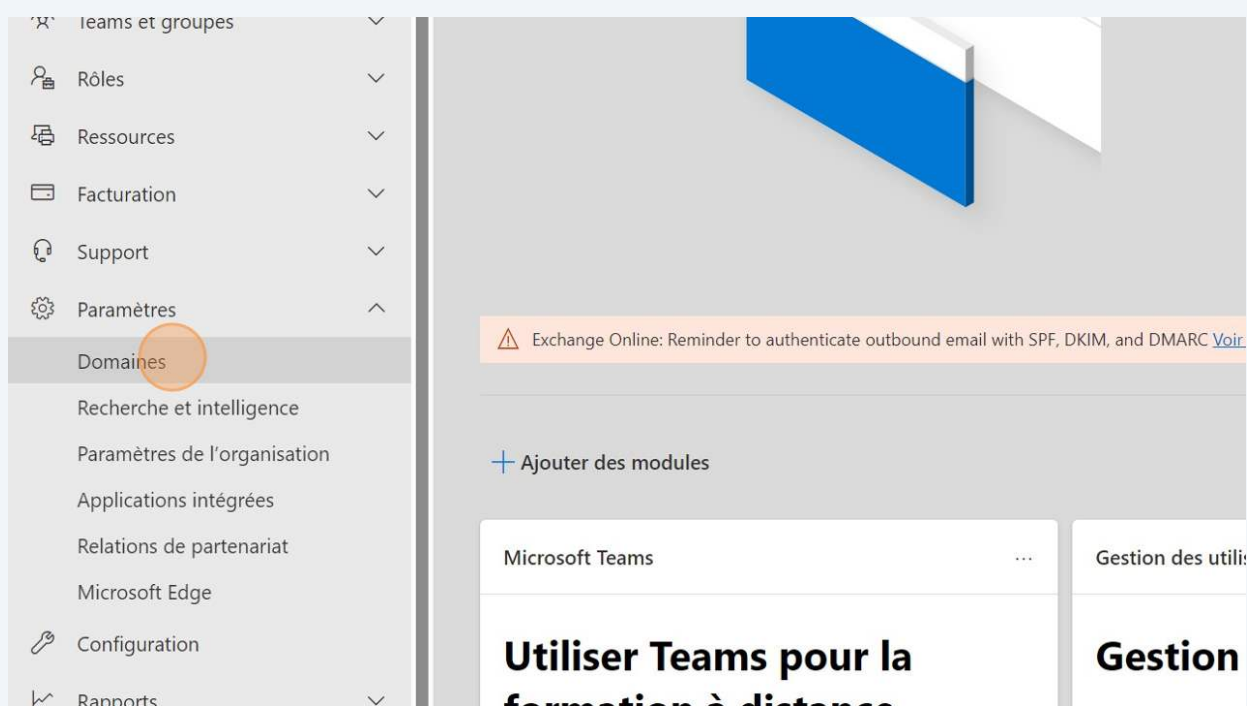
Prévenir le traitement du SPAM en mettant en place SPF, DKIM et DMARC

Nous recevons beaucoup de courrier. Mais à cause de cela, de nombreux courriers importants se retrouvent souvent dans la boîte aux lettres indésirable. Si vous ne faites rien, vous en serez également victime. Empêchez vos courriers de se retrouver dans le SPAM en procédant à quelques réglages de nom de domaine. Pour cela, vous devez ouvrir la gestion DNS de votre nom de domaine et récupérer et vérifier certaines valeurs à partir du centre d'administration Microsoft. (A1, A3, A5)

1

Ouvrez le panneau d'administration <https://admin.microsoft.com>.

Sous "Paramètres", sélectionnez "Domaines"



2

Cliquez sur l'un des noms de domaine (pas le onmicrosoft.com) et choisissez ensuite "Enregistrements DNS" en haut.

The screenshot shows the Microsoft 365 admin center interface. On the left is a navigation pane with various categories. The main content area is titled 'Géré en externe' and includes buttons for 'Définir par défaut', 'Supprimer le domaine', and 'Actualiser'. Below these are tabs for 'Vue d'ensemble', 'Enregistrements DNS' (which is highlighted with an orange circle), 'Utilisateurs', 'Équipes et groupes', and 'Applications'. Under the 'Enregistrements DNS' tab, the 'État du domaine' section shows a green checkmark and the word 'Sain', with a message stating 'Tout semble sain et aucun élément ne nécessite votre attention.'

3

Cliquez sur Gérer les DNS en haut et confirmez en cliquant sur "continuer" jusqu'à ce que vous voyiez les enregistrements DNS.

The screenshot shows the Microsoft 365 admin center interface with the 'Enregistrements DNS' tab selected. Below the tabs, there is a section titled 'Pour gérer les enregistrements DNS pour [domain], accédez à votre fournisseur d'hébergement DNS'. It provides instructions on connecting services to the domain by adding DNS records. Below this, there are buttons for 'Vérifier l'état d'intégrité', 'Gérer DNS' (highlighted with an orange circle), 'Télécharger le fichier CSV', and 'Télécharger le fichier de zone'. At the bottom, there is a section titled 'Microsoft Exchange' with a table of DNS records.

	Type	État	Nom	Valeur
☐	MX		@	0
☐	TXT		@	v=

4

Ouvrez l'enregistrement DNS sous "Microsoft Exchange" de type TXT et cliquez pour copier la valeur TXT.

> **Dossiers CNAME (1)**

✓ **Dossiers TXT (1)**

[Afficher les instructions pour les enregistrements TXT](#)

Enregistrer	Nom TXT	Valeur TXT	Durée de vie
Attendu	@	v=spf1 include:spf.protection.outlook.com -all	1 heure

Options avancées

Précédent

Continuer

5

Dans votre serveur DNS du nom de domaine (externe !), éditez ou créez un nouvel enregistrement de type TXT, laissez le nom vide et collez le contenu. Sauvegardez et attendez quelques minutes/heures.

Votre enregistrement SPF est maintenant défini.

Ajoutez un nouvel enregistrement TXT en fournissant un nom d'hôte et le contenu de l'enregistrement. Un enregistrement TXT peut contenir n'importe quel contenu textuel. Cliquez ensuite sur 'Enregistrer'.

En raison de la mise en cache DNS, cela peut prendre un certain temps avant que ce changement soit visible sur Internet.

Nom

Contenu

"v=spf1 include:spf.protection.outlook.com -all"

Description

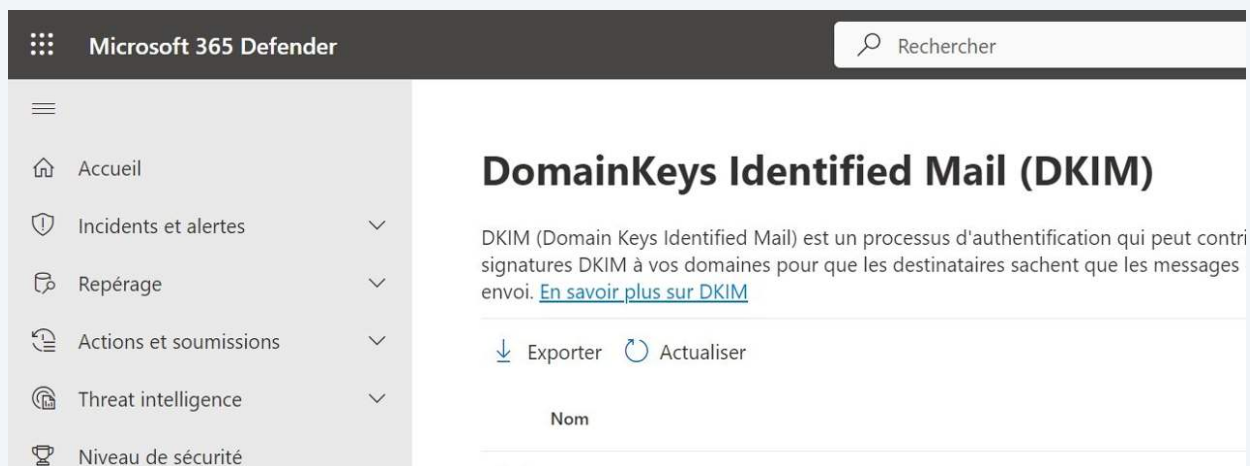
SAUVEGARDER

ANNULER

6

Naviguez vers <https://security.microsoft.com/dkimv2> et cliquez sur le nom de domaine que vous souhaitez activer

(cliquez dessus, ne le cochez pas).



Microsoft 365 Defender

Rechercher

DomainKeys Identified Mail (DKIM)

DKIM (Domain Keys Identified Mail) est un processus d'authentification qui peut contraindre les signatures DKIM à vos domaines pour que les destinataires sachent que les messages envoient. [En savoir plus sur DKIM](#)

Exporter Actualiser

Nom

7

Choisissez d'activer DKIM.



↑ ↓ ×

Signer les courriers pour ce domaine en utilisant des signatures DKIM

☐ Désactivé

État

Aucune signature DKIM n'est utilisée pour ce domaine.

Date de la dernière vérification

2 oct. 2023 12:24:14

8

Dans le message que vous obtenez, copiez le nom et la valeur pour créer le CNAME pour selector1 et selector2.

Domaine accepté

Désactivé

État

Aucune signature DKIM n'est utilisée pour ce domaine

la dernière vérification

14:22:41

Publier les enregistrements CNAME

La synchronisation des clés DKIM peut prendre plusieurs minutes. Ajoutez les enregistrements CNAME suivants auprès de votre fournisseur d'hébergement DNS, puis revenez à cette page pour activer DKIM.

[En savoir plus sur DKIM](#)

Host Name : selector1._domainkey
Points to address or value: selector1-...-..._domainkey.educationtech.onmicrosoft.com

Host Name : selector2._domainkey
Points to address or value: selector2-...-..._domainkey.educationtech.onmicrosoft.com

Copier Fermer

9

Créez le CNAME avec les informations copiées.
Vous faites cela deux fois (Sélecteur1 et Sélecteur2)

Mettre à jour l'enregistrement CNAME

Ajoutez un nouvel enregistrement CNAME en fournissant le nom d'hôte et le nom d'hôte cible. Cliquez ensuite sur 'Enregistrer'.
En raison de la mise en cache DNS, cela peut prendre un certain temps avant que ce changement soit visible sur Internet.

Nom d'hôte
selector1._domainkey

Pointe vers
selector1-...-..._domainkey.educationtech.onmicrosoft.com

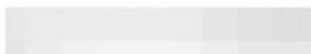
Description

SAUVEGARDER ANNULER

10

Attendez quelques heures/jours et activez à nouveau l'enregistrement DKIM (re-test).

Votre enregistrement DKIM est maintenant défini.



Signer les courriers pour ce domaine en utilisant des signatures DKIM



Désactivé

État

Aucune signature DKIM n'est utilisée pour ce domaine.

Date de la dernière vérification

2 oct. 2023 12:24:14

11

Naviguez vers <https://learn.microsoft.com/fr-fr/microsoft-365/security/office-365-security/email-authentication-dmarc-configure>

Copiez le paramètre DMARC que vous souhaitez configurer.

Utiliser, familiarisez-vous avec les concepts de la section
de DMARC dans Microsoft 365.

"v=DMARC1; p=none"

Copier

re en quarantaine)

"v=DMARC1; p=quarantine"

Copier

Copier

Ressources supplémentaires

Entraînement

Module

[Gérer les stratégies anti-programmes malveillants et anti-courrier indésirable - Training](#)

Gérer les stratégies anti-programmes malveillants et anti-courrier indésirable

Documentation

[Utiliser DKIM pour le courrier électronique dans votre domaine personnalisé](#)

Découvrez comment utiliser DKIM (DomainKeys Identified Mail) avec Microsoft 365 pour vous assurer que les systèmes de messagerie de destination approuvent...

[Configurer SPF pour empêcher l'usurpation d'identité](#)

12

Au niveau de l'hébergement de votre nom de domaine DNS, créez un nouvel enregistrement TXT.

Définissez "__dmarc" comme nom et modifiez le contenu copié pour n'inclure que le contenu entre les signes-".

Votre enregistrement DMARC est maintenant prêt.

Mettre à jour l'enregistrement TXT

Ajoutez un nouvel enregistrement TXT en fournissant un nom d'hôte et le contenu de l'enregistrement. Un enregistrement TXT peut contenir n'importe quel contenu textuel. Cliquez ensuite sur 'Enregistrer'.
En raison de la mise en cache DNS, cela peut prendre un certain temps avant que ce changement soit visible sur Internet.

The record has been updated!

Nom

_dmarc

Contenu

v=DMARC1; p=none

Description

SAUVEGARDER

ANNULER

13

Si vous souhaitez recevoir des courriels de rapport DMARC, collez le contenu DMARC avancé et remplacez les boîtes aux lettres de rapport par un compte de messagerie de surveillance.

Votre enregistrement DMARC est maintenant défini.

Ajoutez un nouvel enregistrement TXT en fournissant un nom d'hôte et le contenu de l'enregistrement. Un enregistrement TXT peut contenir n'importe quel contenu textuel. Cliquez ensuite sur 'Enregistrer'.

En raison de la mise en cache DNS, cela peut prendre un certain temps avant que ce changement soit visible sur Internet.

Nom

_dmarc

Contenu

"v=DMARC1; p=none; pct=100; rua=mailto:i[redacted]n;
ruf=mailto:i[redacted]; fo=1"

Description

SAUVEGAUVER

ANNULER